



PATENT OFFICE  
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy  
of the following application as filed with this office.

Date of Application: April 26, 1999

Application Number: Japanese Patent Application  
No. 11-118072

Applicant(s): NIPPON TELEGRAPH AND TELEPHONE  
CORPORATION

August 30, 1999

Commissioner,  
Patent Office

Takeshi Isayama (Seal)

Certificate No.11-3060105

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

1999年 4月26日

出 願 番 号  
Application Number:

平成11年特許願第118072号

出 願 人  
Applicant (s):

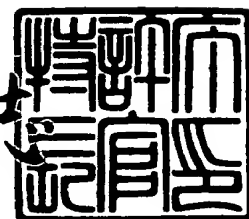
日本電信電話株式会社



1999年 8月30日

特許庁長官  
Commissioner,  
Patent Office

伴佐山建志



出証番号 出証特平11-3060105

【書類名】 特許願

【整理番号】 NTTH107475

【提出日】 平成11年 4月26日

【あて先】 特許庁長官殿

【国際特許分類】 G06C

【発明者】

    【住所又は居所】 東京都新宿区西新宿三丁目 19番2号 日本電信電話株式会社内

    【氏名】 小川 宏

【発明者】

    【住所又は居所】 東京都新宿区西新宿三丁目 19番2号 日本電信電話株式会社内

    【氏名】 中村 高雄

【発明者】

    【住所又は居所】 東京都新宿区西新宿三丁目 19番2号 日本電信電話株式会社内

    【氏名】 富岡 淳樹

【発明者】

    【住所又は居所】 東京都新宿区西新宿三丁目 19番2号 日本電信電話株式会社内

    【氏名】 高嶋 洋一

【特許出願人】

    【識別番号】 000004226

    【氏名又は名称】 日本電信電話株式会社

【代理人】

    【識別番号】 100066153

    【弁理士】

    【氏名又は名称】 草野 卓

【選任した代理人】

【識別番号】 100100642

【弁理士】

【氏名又は名称】 稲垣 稔

【先の出願に基づく優先権主張】

【出願番号】 平成10年特許願第251193号

【出願日】 平成10年 9月 4日

【手数料の表示】

【予納台帳番号】 002897

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9806848

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 抽出電子透かし情報統計処理方法、その装置及びプログラム記憶媒体

【特許請求の範囲】

【請求項1】 情報コンテンツに埋め込まれた電子透かし情報を再構成する方法において、

情報コンテンツから抽出された再構成前の情報系列から、統計学における二項分布に基づく検定方法を用いて、情報コンテンツに埋め込まれていた電子透かし情報を再構成することを特徴とする抽出電子透かし情報統計処理方法。

【請求項2】 請求項1記載の方法において、

抽出した電子透かし情報の信頼度のしきい値 $\alpha$ を予め決めておき、

情報コンテンツから任意に抽出した1ビット系列のビット1又は0の出現確率 $q$ と電子透かしの各ビットの繰り返し回数からそのビット系列に1又は0が $x$ 個含まれる確率を表わす二項分布関数 $F(x)$ を求め、

情報コンテンツの透かし埋め込み対象領域から電子透かし情報の各ビットごとの電子透かし系列 $n_i$ を抽出し、

その抽出した電子透かし系列 $n_i$ に含まれるビット1又は0の数 $k_i$ を計算し、

ビット数 $k_i$ について二項分布関数 $F(x)$ を用いて出現確率 $F(k_i)$ を計算し、

$F(k_i) > \alpha$ であれば $i$ 番目の電子透かし情報 $w_i$ を1又は0に再構成し、

$1 - F(k_i) > \alpha$ であれば電子透かし情報 $w_i$ を0又は1に再構成し、

$F(k_i) > \alpha$ でも、 $1 - F(k_i) > \alpha$ でもなければ電子透かし無しもしくは不明と判定することを特徴とする抽出電子透かし情報統計処理方法。

【請求項3】 請求項2記載の方法において、

再構成した電子透かし情報 $w_i$ が1であれば $F(k_i)$ をその信頼度として出力し、

再構成した電子透かし情報 $w_i$ が0であれば $1 - F(k_i)$ をその信頼度として出力することを特徴とする抽出電子透かし情報統計処理方法。

【請求項4】 請求項1記載の方法において、

抽出した電子透かし情報の信頼度のしきい値 $\alpha$ を決定しておき、

情報コンテンツから任意に抽出した1ビット系列のビット1又は0の出現確率 $q$ と電子透かしの各ビットの繰り返し回数 $t$ から、そのビット系列に1又は0が $x$ 個含まれる確率を表わす二項分布関数 $F(x)$ を求め、

その二項分布関数 $F(x)$ を用いて、その透かし系列が、透かし情報であるか否かを表わす確率を求め、

この確率がしきい値 $\alpha$ を超えているか否かを調べ、超えていれば、情報コンテンツから読み取った透かし系列を多数決処理して電子透かし情報を再構成し、

しきい値 $\alpha$ を超えていなければ、電子透かし無しもしくは不明と判定することを特徴とする抽出電子透かし情報統計処理方法。

【請求項5】 請求項4記載の方法において、

上記再構成した電子透かし情報の信頼度として、上記確率を出力することを特徴とする抽出電子透かし情報統計処理方法。

【請求項6】 請求項1乃至5の何れかに記載の方法において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調することを特徴とする抽出電子透かし情報統計処理方法。

【請求項7】 請求項1記載の方法において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

抽出した電子透かし情報の信頼度のしきい値 $\alpha$ を決定しておき、

情報コンテンツから任意に抽出した1ビット系列のビット1又は0の出現確率 $q$ と電子透かしの各ビットの繰り返し回数 $t$ から、そのビット系列に1又は0が $x$ 個含まれる確率を表わす二項分布関数 $F(x)$ を求めておき、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調されたものを復調し、

出現確率 $q$ を $1/2$ とし、 $0 \leq F(x=x_0) \leq 1-\alpha$ を満たす最大の値 $x_0$ と

、 $\alpha \leq F(x = x_1) \leq 1$  を満す最小の値  $x_1$  とを求めておき、

i 番目に相当する電子透かし系列  $n_i$  に含まれるビット 1 又は 0 の数  $k_i$  を求め、

$k_i \leq x_0$  であれば i 番目の電子透かし情報  $w_i$  を 0 又は 1 に、 $k_i \geq x_1$  であれば電子透かし情報  $w_i$  を 1 又は 0 にそれぞれ再構成することを特徴とする抽出電子透かし情報統計処理方法。

【請求項 8】 請求項 1 記載の方法において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調し、

抽出した電子透かし情報の信頼度のしきい値  $\alpha$  を決定しておき、

情報コンテンツから任意に抽出した 1 ビット系列のビット 1 又は 0 の出現確率  $q$  と電子透かしの各ビットの繰り返し回数  $t$  から、そのビット系列に 1 又は 0 が  $x$  個含まれる確率を表わす二項分布関数  $F(x)$  を求めておき、

上記出現確率  $q$  を  $1/2$  とし、 $0 \leq F(x = x_0) \leq 1 - \alpha$  又は  $\alpha \leq F(x = x_1) \leq 1$  を満す  $x_0$  又は  $x_1$  を求めておき、

透かし系列の二項分布の中心からのかたより度合の平均値が  $x_0$  以下又は  $x_1$  以上であるかを判定し、

$x_0$  以下又は  $x_1$  以上であれば、情報コンテンツから読み取った透かし系列を多数決処理して電子透かし情報を再構成し、

$x_0$  以下又は  $x_1$  以上でなければ電子透かし無しもしくは不明と判定すること

を特徴とする抽出電子透かし情報統計処理方法。

【請求項 9】 請求項 8 記載の方法において、

電子透かし情報を再構成した場合に、上記透かし系列の二項分布の中心からのかたより度合の平均値を、その再構成電子透かし情報の信頼度として出力することを特徴とする抽出電子透かし情報統計処理方法。

【請求項 10】 情報コンテンツに埋め込まれた電子透かし情報を再構成する方法において、

情報コンテンツから任意に抽出した1ビット系列の各ビットの出現確率から得られる二項分布に対する情報コンテンツにおける抽出した再構成前の出現確率の偏りから電子透かし情報を求めることを特徴とする抽出電子透かし情報統計処理方法。

【請求項 11】 情報コンテンツに埋め込まれた電子透かし情報を再構成する装置であって、

情報コンテンツから抽出された再構成前の情報系列から、統計学における二項分布関数  $F(x)$  に基づく検定方法を用いて情報コンテンツに埋め込まれていた電子透かし情報を再構成する抽出手段を有することを特徴とする抽出電子透かし情報統計処理装置。

【請求項 12】 請求項 10 記載の装置において、

上記抽出手段は、情報コンテンツから任意に抽出した1ビット系列の各ビットの出現確率と電子透かしの各ビットの繰り返し回数から二項分布関数  $F(x)$  を求める手段と、

上記電子透かし情報の各ビット値ごとに電子透かし系列を抽出する手段と、

上記抽出した電子透かし系列の出現確率を、上記求めた二項分布関数  $F(x)$  から求める手段と、

その求めた出現確率又は  $1 - \text{出現確率}$  が信頼度のしきい値より大きいかな否かを判定する手段と、

上記しきい値より大きいと判定された情報について電子透かし情報を再構成する手段とよりなることを特徴とする抽出電子透かし情報統計処理装置。

【請求項 13】 請求項 12 記載の装置において、

上記求めた出現確率から、上記再構成した情報ビットについての信頼度を求めて、その再構成情報ビットと共に出力する手段を備えることを特徴とする抽出電子透かし情報統計処理装置。

【請求項 14】 請求項 11 記載の装置において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

抽出した電子透かし情報の信頼度のしきい値  $\alpha$  が決定されており、



情報コンテンツから任意に抽出した1ビット系列のビット1又は0の出現確率 $q$ と電子透かしの各ビットの繰り返し回数 $t$ から、そのビット系列に1又は0が $x$ 個含まれる確率を表わす二項分布関数 $F(x)$ が求められてあり、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調する手段と、

上記抽出手段は、

$i$ 番目に相当する電子透かし系列 $n_i$ に含まれるビット1又は0の数 $k_i$ を求める手段と、

出現確率 $q$ を $1/2$ とし、 $0 \leq F(x=x_0) \leq 1-\alpha$ を満す最大の値 $x_0$ と $k_i$ を比較し、 $k_i \leq x_0$ であれば、 $i$ 番目の電子透かし情報 $w_i$ を0又は1に再構成し、 $\alpha \leq F(x=x_1) \leq 1$ を満す最小の値 $x_1$ と $k_i$ を比較し、 $k_i \geq x_1$ であれば $i$ 番目の電子透かし情報 $w_i$ を1又は0に再構成する手段とよりなることを特徴とする抽出電子透かし情報統計処理装置。

【請求項15】 請求項11記載の装置において、

抽出した電子透かし情報の信頼度のしきい値 $\alpha$ が決定されており、

情報コンテンツから任意に抽出した1ビット系列のビット1又は0の出現確率 $q$ と電子透かしの各ビットの繰り返し回数 $t$ から、そのビット系列に1又は0が $x$ 個含まれる確率を表わす二項分布関数 $F(x)$ を求める手段と、

その二項分布関数 $F(x)$ を用いて、その透かし系列が、透かし情報であるか否かを表わす確率を求める手段と、

この確率がしきい値 $\alpha$ を超えているか否かを調べる判定手段と、

その判定手段でしきい値を超えていると判定されると、情報コンテンツから読み取った透かし系列を多数決処理して電子透かし情報を再構成する手段と、

上記判定手段でしきい値 $\alpha$ を超えていないと判定されると、電子透かし無しもしくは不明と判定する手段とを備えることを特徴とする抽出電子透かし情報統計処理装置。

【請求項16】 請求項15記載の装置において、

上記再構成した電子透かし情報の信頼度として、上記確率を出力する手段を備えることを特徴とする抽出電子透かし情報統計処理装置。

【請求項 1 7】 請求項 1 1、1 3、1 5、1 6 の何れかに記載の装置において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調する手段を備えることを特徴とする抽出電子透かし情報統計処理装置。

【請求項 1 8】 請求項 1 1 記載の装置において、

抽出した電子透かし情報の信頼度のしきい値  $\alpha$  が決定されており、

情報コンテンツから任意に抽出した 1 ビット系列のビット 1 又は 0 の出現確率  $q$  と電子透かしの各ビットの繰り返し回数  $t$  から、そのビット系列に 1 又は 0 が  $x$  個含まれる確率を表わす二項分布関数  $F(x)$  が求められてあり、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調する手段と、

上記抽出手段は、

上記出現確率  $q$  を  $1/2$  とし、 $0 \leq F(x = x_0) \leq 1 - \alpha$  又は  $\alpha \leq F(x = x_1) \leq 1$  を満す  $x_0$  又は  $x_1$  と透かし系列の二項分布の中心からのかたより度合の平均値とを比較し、その平均値が  $x_0$  以下又は  $x_1$  以上であるかを判定する手段と、

その判定が  $x_0$  以下又は  $x_1$  以上であれば、情報コンテンツから読み取った透かし系列を多数決処理して電子透かし情報を再構成する手段と、

$x_0$  以下又は  $x_1$  以上でなければ電子透かし無しもしくは不明と判定する手段とよりなることを特徴とする抽出電子透かし情報統計処理装置。

【請求項 1 9】 請求項 1 7 記載の装置において、

電子透かし情報が再構成されると、上記透かし系列の二項分布の中心からのかたより度合の平均値を、その再構成電子透かし情報の信頼度として出力する手段を備えることを特徴とする抽出電子透かし情報統計処理装置。

【請求項 2 0】 情報コンテンツに埋め込まれた電子透かし情報を再構成す

るプログラムを格納した記憶媒体であって、

情報コンテンツから抽出された再構成前の情報系列から、統計学における二項分布に基づく検定方法を用いて情報コンテンツに埋め込まれていた電子透かし情報を再構成する処理を

コンピュータが実行することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項 21】 請求項 20 記載の記憶媒体において、

抽出した電子透かし情報の信頼度のしきい値  $\alpha$  が予め決められてあり、

上記電子透かし情報を再構成する処理は、

情報コンテンツから任意に抽出した 1 ビット系列のビット 1 又は 0 の出現確率  $q$  と電子透かしの各ビットの繰り返し回数からそのビット系列に 1 又は 0 が  $x$  個含まれる確率を表わす二項分布関数  $F(x)$  を求める処理と、

情報コンテンツの透かし埋め込み対象領域から電子透かし情報の各ビットごとの電子透かし系列  $n_i$  を抽出する処理と、

その抽出した電子透かし系列  $n_i$  に含まれるビット 1 又は 0 の数  $k_i$  を計算する処理と、

ビット数  $k_i$  について二項分布関数  $F(x)$  を用いて出現確率  $F(k_i)$  を計算する処理と、

$F(k_i) > \alpha$  であれば  $i$  番目の電子透かし情報  $w_i$  を 1 又は 0 に再構成する処理と、

$1 - F(k_i) > \alpha$  であれば電子透かし情報  $w_i$  を 0 又は 1 に再構成する処理と、

$F(k_i) > \alpha$  でも、 $1 - F(k_i) > \alpha$  でもなければ電子透かし無しもしくは不明と判定する処理とよりなることを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項 22】 請求項 21 記載の記憶媒体において、

再構成した電子透かし情報  $w_i$  が 1 であれば  $F(k_i)$  をその信頼度として出力し、

再構成した電子透かし情報  $w_i$  が 0 であれば  $1 - F(k_i)$  をその信頼度とし

て出力する処理を上記コンピュータが実行することを特徴とする抽出電子透かし情報統計処理プログラム記憶媒体。

【請求項 23】 請求項 20 記載の記憶媒体において、  
抽出した電子透かし情報の信頼度のしきい値  $\alpha$  が決定されており、  
上記電子透かし情報を再構成する処理は、  
情報コンテンツから任意に抽出した 1 ビット系列のビット 1 又は 0 の出現確率  $q$  と電子透かしの各ビットの繰り返し回数  $t$  から、そのビット系列に 1 又は 0 が  $x$  個含まれる確率を表わす二項分布関数  $F(x)$  を求める処理と、  
その二項分布関数  $F(x)$  を用いて、その透かし系列が、透かし情報であるか否かを表わす確率を求める処理と、  
この確率がしきい値  $\alpha$  を超えているか否かを調べる処理と、  
しきい値  $\alpha$  を超えていれば、情報コンテンツから読み取った透かし系列を多数決処理して電子透かし情報を再構成する処理と、  
しきい値  $\alpha$  を超えていなければ、電子透かし無しもしくは不明と判定する処理とよりなることを特徴とする抽出電子透かし情報統計処理プログラム記憶媒体。

【請求項 24】 請求項 23 記載の記憶媒体において、  
上記再構成した電子透かし情報の信頼度として、上記確率を出力する処理を上記コンピュータが実行することを特徴とする抽出電子透かし情報統計処理プログラム記憶媒体。

【請求項 25】 請求項 20 乃至 24 の何れかに記載の記憶媒体において、  
上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、  
電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調する処理を上記コンピュータが実行することを特徴とする抽出電子透かし情報統計処理プログラム記憶媒体。

【請求項 26】 請求項 20 記載の記憶媒体において、  
上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、  
抽出した電子透かし情報の信頼度のしきい値  $\alpha$  が決定されており、

情報コンテンツから任意に抽出した1ビット系列のビット1又は0の出現確率 $q$ と電子透かしの各ビットの繰り返し回数 $t$ から、そのビット系列に1又は0が $x$ 個含まれる確率を表わす二項分布関数 $F(x)$ が求められてあり、

上記電子透かし情報を再構成する処理は、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調されたものを復調する処理と、

$i$ 番目に相当する電子透かし系列 $n_i$ に含まれるビット1又は0の数 $k_i$ を求める処理と、

$k_i$ が、出現確率 $q$ を $1/2$ とし、 $0 \leq F(x=x_0) \leq 1-\alpha$ を満す最大の値 $x_0$ 以下であれば $i$ 番目の電子透かし情報 $w_i$ を0又は1に再構成する処理と、

$k_i$ が、出現確率 $q$ を $1/2$ とし、 $\alpha \leq F(x=x_1) \leq 1$ を満す最小の値 $x_1$ 以上であれば電子透かし情報 $w_i$ を1又は0に再構成する処理とよりなることを特徴とする抽出電子透かし情報統計処理プログラム記憶媒体。

【請求項27】 請求項20記載の記憶媒体において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

抽出した電子透かし情報の信頼度のしきい値 $\alpha$ が決定されてあり、

情報コンテンツから任意に抽出した1ビット系列のビット1又は0の出現確率 $q$ と電子透かしの各ビットの繰り返し回数 $t$ から、そのビット系列に1又は0が $x$ 個含まれる確率を表わす二項分布関数 $F(x)$ が求められてあり、

上記出現確率 $q$ を $1/2$ とし、 $0 \leq F(x=x_0) \leq 1-\alpha$ 又は $\alpha \leq F(x=x_1) \leq 1$ を満す $x_0$ 又は $x_1$ が求められてあり、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調する処理と、

透かし系列の二項分布の中心からのかたより度合の平均値が $x_0$ 以下又は $x_1$ 以上であるかを判定する処理と、

$x_0$ 以下又は $x_1$ 以上と判定されると、情報コンテンツから読み取った透かし系列を多数決処理して電子透かし情報を再構成する処理と、

$x_0$  以下又は  $x_1$  以上でないと判定されると電子透かし無しもしくは不明と判定する処理とを上記コンピュータが実行することを特徴とする抽出電子透かし情報統計処理プログラム記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

マルチメディア著作物は、不正複製や改竄（かいざん）が容易であることから、情報利用者の正当な二次利用やコンテンツ提供者の情報発信の障害となっており、その著作権保護が訴えられている。画像や音声などのメディアの冗長性を利用し、人間に知覚されないように主情報である情報コンテンツに別の副情報を埋め込む技術に『電子透かし技術』がある。この技術は、重畳した情報の分離が困難なことより、マルチメディア著作物の著作権保護に有効な手段として考えられている。この発明は、電子透かしを用いたシステムにおける、抽出透かし情報の統計処理に関する方法及びその装置及び抽出情報の統計処理プログラムを格納した記憶媒体に関するものである。

【0002】

【従来の技術】

特願平8-305370もしくは特願平8-338769もしくは特願平9-9812もしくは特願平9-14388もしくは特願平9-57516もしくは特願平9-109924もしくは特願平9-164466もしくは特願平9-197003もしくは特願平9-218467もしくは特願平10-33239などに記載の電子透かし技術（Digital Watermark, Data Hiding, Finger Printing, Steganography, 画像・音声深層暗号などとも呼ぶ）を用いたシステムにおいて一番重要な問題は、埋め込んだ情報の有無の判定および埋め込んだ情報の信頼性の精度である。電子透かしシステムは、電子透かしを埋め込んだ情報コンテンツに対する様々なメディア処理を想定して、情報コンテンツに埋め込まれている副情報（以下電子透かし情報と呼ぶことにする）がある程度壊れていても、正しい電子透かし情報を再構成する機構を持っているものが一般的である。しかしながら現状は、

再構成した透かし情報の正当性を定量評価できないものがほとんどであり、信頼性に欠けるものであった。

【0003】

【発明が解決しようとする課題】

電子透かし情報を読みとった際に起こる問題である、電子透かしが入っていない情報コンテンツを電子透かし有りと判定したり、電子透かしが入っている情報コンテンツから正しくない電子透かしを抽出する確率を定量的に評価できる方法、装置、プログラム記憶媒体を提供することをこの発明は目的とする。

【0004】

【課題を解決するための手段】

電子透かし処理は、電子透かし埋め込み・電子透かし抽出の対から成る。電子透かし埋め込み処理では、秘密鍵情報などを用いて、情報コンテンツ内の電子透かし対象領域Aから電子透かし埋め込み領域 $B \subseteq A$ を選定し、固有の規則で領域B内のデータを変更する。電子透かし抽出処理では、電子透かし埋め込み領域Bのデータを解釈し、電子透かし情報を再構成する。この発明では、電子透かしが埋め込まれている情報コンテンツにおいて、この発明適用対象となる電子透かしアルゴリズムを用いて、電子透かし対象領域の全体であるAから正誤を問わず任意の秘密鍵情報を用いて読みとられる電子透かし情報の統計学における二項分布をもとに、正しい秘密鍵情報を用いて透かし埋め込み領域Bから読みとられた電子透かし情報がどの程度確率的に起こり得るのかを判定する。

作用

この発明によれば、電子透かし技術において、情報コンテンツから読みとった透かし情報の信頼性を定量的に評価でき、電子透かしが入っていない情報コンテンツを有りと判断したり、電子透かしが入っている情報コンテンツから正しくない電子透かしを読みとったりする確率を一定の値で抑えることができる。

【0005】

【発明の実施の形態】

実施例 1

予め意味が曖昧な言葉の定義を行なっておく。

電子透かし系列とは、情報コンテンツから読み出された再構成処理を行なう以前の情報系列を表し、電子透かし情報とは、情報コンテンツに本当に重畳したい、システムの運用上意味ある情報、もしくは、電子透かし系列を再構成処理し得られる情報を表すものとする。電子透かしの信頼度 $\alpha$ とは、抽出した電子透かしの正当性を表す指標である。すなわち、抽出した電子透かしが、実際に画像に埋め込んでいた電子透かしと一致する確率である。逆に、電子透かしが埋め込まれていない画像から電子透かしを抽出したり、誤った電子透かし情報を抽出する確率を信頼度 $\alpha$ を用いて $2(1-\alpha)$ と表現できる。

## 【0006】

同様に埋め込み系列とは、実際に埋め込まれる情報を表し、埋め込み情報を変調したり、引き伸ばしたり、繰り返したりしている系列になっている。

以下にこの発明の実施例1を図面を参照して説明する。

図1は、この発明の背景となる電子透かしシステムの概要図である。

電子透かし情報101は、電子透かし埋め込み装置102によって情報コンテンツ103に埋め込まれ、電子透かし入り情報コンテンツ104に変換される。

## 【0007】

電子透かし入り情報コンテンツ104は、無線・有線・パッケージ媒体などで流通する間に、情報圧縮やメディア処理などによって品質劣化した電子透かし入り情報コンテンツ105に変化する。

この発明の要部である電子透かし情報再構成装置106は電子透かし抽出装置107内部に実装され、電子透かし抽出装置107を用いて、劣化した電子透かし入り情報コンテンツ105から読みとった電子透かし系列を、電子透かし情報再構成装置106を用いて処理し、抽出電子透かし情報108を抽出するという構成になる。

## 【0008】

以上が電子透かし埋め込み・抽出手順の概要である。

以下、電子透かし情報再構成処理の動作を詳細に説明する。

図2は、電子透かし抽出装置107の内部に実装された電子透かし情報再構成装置106の概要である。



電子透かし情報再構成装置106は、電子透かし抽出装置107を利用して、電子透かし情報の全埋め込み対象領域から任意の1ビット電子透かし系列を抽出したときにビット1が抽出される確率 $q$ を予め求めておく。

【0009】

すなわち、1ビット電子透かし系列抽出処理部201のようなものを仮定し、電子透かし対象領域の全要素に対して1ビットずつ電子透かし系列の抽出を行ない（破線L1）、この全試行のうちビット1が何回取り出されたかの率を計算する。

この実施例ではビット1の抽出確率および個数を求めているが、ビット0の抽出確率および個数を求めても実装上の違いのみであり、本質的に変わらないことを留意しておく。

【0010】

これより、電子透かしアルゴリズムを用いて、情報コンテンツ105の電子透かし対象領域から無作為に1ビット電子透かし系列の抽出を行なったときのビット0と1の出現確率はそれぞれ $1-q$ および $q$ と計算される。

$n$ ビット電子透かし系列抽出処理装置202は、電子透かしが埋め込まれている情報コンテンツから電子透かしが埋め込まれたのべ回数だけ電子透かし系列の抽出を行なう。

【0011】

ここで、電子透かし情報を $b_0, b_1, \dots, b_{m-1}$ ,  $b_i \in \{0, 1\}$ ,  $i < m$ （情報長 $m$ ビット）、 $i$ ビット目の電子透かし情報を情報コンテンツに埋め込んだ繰り返し回数（拡散率、chip-rateなどとも呼ぶ）を $n_i$ 回、読みとった電子透かし系列を

$$\begin{aligned} & b'_{0,0}, b'_{0,1}, \dots, b'_{0,n_0-1}, b'_{1,0}, b'_{1,1}, \dots, b'_{1,n_1-1}, \dots \\ & b'_{m-1,0}, b'_{m-1,1}, \dots, b'_{m-1,n_{m-1}-1} \\ & b'_{i,j} \in \{0, 1\} \end{aligned}$$

（長さ $\sum_{r=0}^{m-1} n_r$ ビット列）と定義する。

【0012】

電子透かし情報再構成装置106は、 $n$ ビット電子透かし情報抽出処理部20

2 から、電子透かし情報の 0 番目に相当する電子透かし系列の部分列から  $m-1$  番目に相当する電子透かし系列の部分列までを順次入力として受けとる（実線 L2）。

次に、実際に電子透かし情報の  $i$  ビット目の電子透かし情報を再構成する方法を具体的に述べる。

【0013】

電子透かし対象領域から任意に  $n_i$  ビット電子透かし系列の抽出を行なったとき、この  $n_i$  ビット列にビット 1 が  $k$  個現れる確率  $P(x=k)$  は、二項分布の密度関数によって

$$P(x=k) = n_i C_k q^k \cdot (1-q)^{n_i-k} \quad (1)$$

で表され、その分布関数  $F(x)$  は、

$$F(x) = \sum_{k=0}^x n_i C_k q^k \cdot (1-q)^{n_i-k} \quad (2)$$

$$(0 \leq x \leq n_i)$$

である。ただし、 $n_i C_k$  は、 $n_i$  個の中から  $k$  個のものを選ぶ組合せ数を表す。

【0014】

電子透かし情報の信頼度のしきい値  $\alpha$  ( $1/2 < \alpha \leq 1$ ) を設け、電子透かし情報再構成装置 106 に入力された電子透かし情報の  $i$  番目に相当する電子透かし系列の部分列  $b'_{i,0} b'_{i,1} \dots b'_{i,n_i-1}$  に含まれるビット 1 の数を

$$k_i = \sum_{r=0}^{n_i-1} b'_{i,r}$$

によって計算し、式 (2) を用いて電子透かし情報を

$$b_i = \begin{cases} 0 & 0 \leq F(k_i) \leq 1-\alpha \text{ のとき} \\ 1 & \alpha \leq F(k_i) \leq 1 \text{ のとき} \\ \text{不明もしくは無し} & 1-\alpha < F(k_i) < \alpha \text{ のとき} \end{cases} \quad (3)$$

と判定する。

【0015】

見方を変えて電子透かし系列  $n_i$  に含まれるビット 1 の個数によって判定すると、 $0 \leq F(x=x_0) \leq 1-\alpha$  を満たす最大の  $x_0$  と、 $\alpha \leq F(x=x_1) \leq 1$  を満たす最小の  $x_1$  をしきい値として、図 3 に示すように  $n_i$  個中の 1 が  $x_0$

以下なら 0 と、 $x_1$  以上なら 1 と透かし情報を判定する。

図 3 の横軸は電子透かし系列に含まれるビット 1 の個数、縦軸はその出現頻度を表す。電子透かしが埋め込まれていない情報コンテンツではその任意に抽出したビット系列中に 1 が出現する頻度は二項分布となりその系列のビット数  $n$  の半分の所がピークとなる。しかし電子透かし情報が埋め込まれた部分では電子透かし情報のビット 0 が埋め込まれた部分列  $n_i$  についてはビット 1 の出現頻度は、品質劣化がない場合は 0 であり、品質劣化があっても、小さな値、つまり  $x_0$  以下であり、電子透かし情報のビット 1 が埋め込まれた部分列  $n_i$  についてはビット 1 の出現頻度は、品質劣化がない場合は、 $n/2$  であり、品質劣化があっても大きな値  $x_1$  以上である。このように電子透かし情報が埋め込まれた電子透かし系列のビット 1 又は 0 の出現頻度は、二項分布に対し分布の中心が、偏ったものとなり、この発明ではこの偏りを利用して電子透かし情報を、抽出した電子透かし系列から再構成する。

#### 【0016】

電子透かしシステムによっては、情報コンテンツ 105 から抽出された電子透かし系列の分布  $P(x)$  の中心値に対する偏りから再構成した電子透かし情報を求め、抽出された電子透かし系列が統計的にどの程度の確率で出現するのかを式 (2) の値で求めて、再構成された電子透かし情報が 1 の場合は  $F(k_i)$  を、情報が 0 の場合は  $1 - F(k_i)$  を電子透かしの信頼度として付加して出力することも可能である。この電子透かしの信頼度  $F(k_i)$ 、 $1 - F(k_i)$  は、情報コンテンツから任意に抽出した 1 ビット系列の各ビットの出現確率から得られる二項分布に対する情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の偏りから求めたものになる。

#### 【0017】

この処理を電子透かし情報の情報長  $m$  ビットに拡張した概念を図 4 に示す。

電子透かし情報再構成装置 106 は、再構成した電子透かし情報  $b_0, b_1, \dots, b_{m-1}$  を抽出電子透かし情報 108 として出力する。

以上が電子透かし情報再構成処理の動作についてである。

この処理の手順を図 5 に示す。電子透かし入り情報コンテンツ 105 と、電子

透かし情報抽出に必要な秘密情報が入力され、その情報コンテンツ 105 と秘密情報とを用いて、各ビット値に関して、電子透かし系列を抽出する (S1)。透かしの信頼度のしきい値  $\alpha$  を設定し (S2)、電子透かし情報のすべての埋め込み対象領域から透かしを任意に 1 ビット読み取ったときのビットが 1 である確率  $q$  を求める (S3)。この確率  $q$  と電子透かしの各ビットの繰り返し回数  $n_i$  とからビット系列に 1 が  $x$  個含まれる確率を表わす二項分布関数  $F(x)$  を求める (S4)。

## 【0018】

電子透かし系列の部分列を区別する  $i$  を 0 とし (S5)、その部分列中のビットが 1 の個数  $k_i = \sum_{j=0}^{n_i-1} b'_{i,j}$  を求め、その出現確率  $F(k_i)$  を求め、これが  $1-\alpha$  以下であるかを調べる (S6)、 $F(k_i) \leq 1-\alpha$  であれば電子透かし情報  $w'_i$  を 0 に再構成 (S7)、 $i$  を +1 し (S8)、 $i < m$  ならステップ S6 に戻る (S9)。ステップ S6 で  $F(k_i) \leq 1-\alpha$  でなければ  $F(k_i) \geq \alpha$  が成立するかを調べ (S10)、成立すれば電子透かし情報  $w_i$  を 1 に再構成してステップ S8 に移る (S11)。ステップ S10 で  $F(k_i) \geq \alpha$  でなければ電子透かし無しもしくは不明と判定して処理を終了する (S12)。ステップ S9 で  $i$  が  $n_i$  より大となれば再構成された電子透かし系列  $\{w'_i\}$  を出力する。なおステップ S1 の各ビット値に関して電子透かし系列の抽出はステップ S4 と S5 との間で行ってもよい。ステップ S6、S10 でそれぞれ  $1-F(k_i)$ 、 $F(k_i)$  が  $\alpha$  より大であるかを判定している。

## 【0019】

実施例 1 では、式 (1) に表される分布に偏りが無い、つまり、 $q \simeq 1/2$  となることを前提としている。

電子透かし情報のそれぞれのビット埋め込み回数  $n_i$  が、統計的特徴を得るのに十分な数である場合、一般的には、 $q \simeq 1/2$  となるが、 $q$  の値は、電子透かしアルゴリズムと情報コンテンツの特徴に依存するため、稀に  $q$  が  $1/2$  から大きく外れた数となることがある。

## 【0020】

この問題を回避する方法を実施例 2 で示す。

## 実施例 2

以下にこの発明の実施例 2 を図面を参照して説明する。

図 6 は、この実施例 2 を付加した電子透かしシステムの概要図である。

電子透かし埋め込み装置 1 0 2 が情報コンテンツ 1 0 3 に電子透かし情報 1 0 1 を埋め込む際に、電子透かし情報の各ビット値を  $n_i$  回繰り返して埋め込む処理において、電子透かし埋め込み装置 1 0 2 の内部に実装された疑似乱数系列発生器（甲） 5 0 1 を用いて、埋め込み系列を変調し、これを情報コンテンツ 1 0 3 に埋め込む。

【0 0 2 1】

例えば、埋め込み系列を

$$b_{0,0} b_{0,1} \cdots b_{0,n_0-1} b_{1,0} b_{1,1} \cdots b_{1,n_1-1} \cdots b_{m-1,0} b_{m-1,1} \cdots b_{m-1,n_{m-1}-1}$$

$$b_{i,j} \in \{0, 1\}$$

疑似乱数系列を

$$r_{i,0} r_{i,1} \cdots r_{i,n_i-1}$$

$$r_{i,j} \in \{0, 1\}$$

とおくと、埋め込み系列を疑似乱数系列によって

$$m_{i,0} m_{i,1} \cdots m_{i,n_i-1}$$

$$m_{i,j} = b_{i,j} (+) r_{i,j}$$

に変調する。A (+) B は A と B の排他的論理和を表わす。

【0 0 2 2】

この処理により、電子透かし抽出処理には、電子透かし系列埋め込みに用いたのと同じ疑似乱数系列が必要となる。

例えば、疑似乱数系列として M 系列を用いたとする。

すると、任意の M 系列を用いて 1 ビット電子透かし系列抽出を行なったとき  $q \simeq 1/2$  となり、電子透かしアルゴリズムと情報コンテンツに依存することなくこの発明を適用可能となる。

【0 0 2 3】

電子透かし抽出では、電子透かし抽出装置 1 0 7 の内部に実装された疑似乱数系列発生器（乙） 5 0 2 を用いて、

$$b'_{i,j} = m_{i,j} (+) r_{i,j}$$

により復調する。

ここで、疑似乱数発生器（甲）501と疑似乱数発生器（乙）502は、同じ疑似乱数系列を発生するように実装する必要がある。

【0024】

復調処理により得られた電子透かし系列

$$\begin{aligned} & b'_{0,0} \ b'_{0,1} \ \cdots \ b'_{0,n0-1} \ b'_{1,0} \ b'_{1,1} \ \cdots \ b'_{1,n1-1} \ \cdots \\ & b'_{m-1,0} \ b'_{m-1,1} \ \cdots \ b'_{m-1,nm-1-1} \\ & b'_{i,j} \in \{0, 1\} \end{aligned}$$

に対して、実施例1で説明した方法により電子透かし情報を再構成する。

【0025】

読みとった電子透かし系列のビット1の出現確率 $q$ は、変調の有無に関わらず二項分布に近似できると考えられるため、この実施例で示した変調処理による密度関数の分布(1)への影響はない。

また、実装において、 $q = 1/2$ と仮定できるため、つまり $q$ を求める処理(201)を行うことなく、式(2)で $q = 1/2$ として計算することにより、電子透かし情報再構成処理は多数決処理と同程度の計算量となり、高速化が図れる。

### 実施例3

実施例3では、実施例1および実施例2で示した発明の例に基づき、実際に数値を示して例を説明する。ここでは電子透かし情報を1ビットとし、その埋め込み繰り返し回数 $n$ を127回とし、電子透かし情報の全埋め込み対象領域から任意の1ビット電子透かし系列を抽出したときにビット1が抽出される確率 $q$ を $1/2$ とする。信頼性のしきい値 $\alpha$ を0.99999(99.999%の意)とすると、図3における $x_0$ は36、 $x_1$ は90である。すなわち、以上の条件の下でこの発明は、電子透かし情報を、電子透かし系列( $n$ ビット)に現れる1の個数が36以下である場合はビット0、90以上の場合はビット1、それ以外の場合は電子透かしが不明もしくは無しと判定する。電子透かし情報有りとは判定した場合、その正当率は99.999%以上を保証できる。

実施例 4

図 5 に示した実施例ではその処理手順から理解されるように、電子透かし情報の 1 ビットでも信頼性が得られない、つまり  $F(k_i)$  又は  $1 - F(k_i)$  が  $\alpha$  より小さなものになれば電子透かしなし、又は不明となり、電子透かし情報の再構成は不能となる。この実施例 4 はこのような問題を解決したものである。この場合は電子透かし情報の各ビットの埋め込み繰り返し回数は同一値  $n$  とする。

## 【0026】

以下、情報コンテンツから読み取られた透かし系列  $b'_{0,0}, b'_{0,1}, \dots, b'_{0,n-1}, b'_{1,0}, b'_{1,1}, \dots, b'_{1,n-1}, b'_{m,0}, b'_{m,1}, \dots, b'_{m,n-1}$  から透かし情報  $w_0, w_1, \dots, w_{m-1}$  を再構成する方法を詳細に述べる (図 7 参照)。

Step 1. まず情報コンテンツと電子透かし情報抽出に必要な秘密情報とから各ビット値に関して電子透かし系列を抽出する。

## 【0027】

Step 2. 透かし情報の信頼度のしきい値  $\alpha$  ( $1/2 < \alpha \leq 1$ ) を設定する。例えば、抽出した透かしの信頼度を 99% 以上に設定したい場合は、 $\alpha = 0.99$  とする。

Step 3. 電子透かし情報のすべての埋め込み対象領域から透かし系列を任意に 1 ビット読み取ったときに、それがビット '1' である確率  $q$  を予め求める。すなわち、電子透かし抽出対象から無作為に電子透かし系列の抽出を行なったときのビット '0' と '1' の出現確率は  $1 - q$  および  $q$  と計算される。

## 【0028】

Step 4. 透かしの各ビット情報を構成する透かし系列にビット '1' が  $x$  個含まれる確率は、二項分布関数  $F(x)$  を用いて、

$$F(x) = \sum_{j=0}^x {}_n C_j q^j \cdot (1-q)^{n-j}$$

と表せる。

Step 5.  $n$  ビットの透かし系列について、電子透かし情報であるかを表す確率がしきい値  $\alpha$  を超えているか、つまり下記の式 (4) を満すかを調べる。

【0029】

【数1】

$$F\left(\frac{\sum_{i=0}^{m-1} \left| \sum_{j=0}^{n-1} b'_{i,j} - \frac{n}{2} \right|}{m} + \frac{n}{2}\right) \geq \alpha \quad \dots\dots (4)$$

なお  $|a|$  は  $a$  の絶対値を表わす。 $\sum_{j=0}^{n-1} b_{i,j} - n/2$  はその  $n$  ビットの透かし系列の 1 ビットの個数の二項分布の中心からの偏りを表わし、その  $\sum_{i=0}^{m-1}$  を  $m$  で割ることは、全電子透かし情報の  $m$  ビットについての平均であり、 $n/2$  は二項分布の中心である。

【0030】

この式 (4) が  $\alpha$  より大であれば、透かし有りであり、よって各  $n$  ビットの透かし系列の  $m$  個についてそれぞれ多数決処理により電子透かし情報を再構成すればよい。

【0031】

Step 6. つまり、透かし有りと判定されると、すべての  $0 \leq i < m$  に対して、

$$\sum_{j=0}^{n-1} b_{i,j} < n/2 \text{ のとき: } w'_i = 0$$

$$\sum_{j=0}^{n-1} b_{i,j} \geq n/2 \text{ のとき: } w'_i = 1$$

により透かし情報を再構成する。図の中 7S6-1 ~ S6-7 によりこの処理が行われる。

Step 7.

【0032】

【数2】

$$F\left(\frac{\sum_{i=0}^{m-1} \left| \sum_{j=0}^{n-1} b_{i,j} - \frac{n}{2} \right|}{m} + \frac{n}{2}\right) < \alpha$$

のとき、透かし無しもしくは不明と判定する。ただし、 $|x|$  は  $x$  の絶対値を表



す。

透かしがあるかの判定式としては式 (4) の代りに次の式 (5) を用いてもよい。

【0 0 3 3】

【数 3】

$$F\left(\frac{n}{2} - \frac{\sum_{i=0}^{m-1} \left| \sum_{j=0}^{n-1} b'_{i,j} - \frac{n}{2} \right|}{m}\right) \leq 1 - \alpha \quad \dots\dots (5)$$

式 (5) の左辺が  $1 - \alpha$  より大きければ透かし無しもしくは不明と判定する。

この実施例 4 では以上の説明から明らかなように、式 (4) 又は式 (5) により、電子透かし情報系列の全体について統計的処理して透かしの有無を判定し、透かしありと判定されると、多数決処理により再構成を行うため、1 ビットでも信頼度が小さいものが存在するために、電子透かし情報の再構成が不能になるようなことはない。

【0 0 3 4】

図 7 において、ステップ S 1 の電子透かし系列抽出を、ステップ S 4 と S 5 の間で行ってもよい。

この実施例 4 についても、実施例 2 で述べたように、電子透かし埋め込み系列に対し、疑似乱数系列で変調して情報コンテンツに対する埋め込みを行い、情報再構成する際に、取り出した透かし系列に対し、疑似乱数系列で復調し、その復調した系列について、式 (4) の判定を行い、その結果  $\alpha$  より大で透かしありと判定されると、復調系列に対し、実施例 4 の S t e p 6 と同様な処理、つまり多数決処理により再構成を行うようにすることもできる。この全体の処理手順を図 8 に図 7 と対応する部分に同一符号を付けて示す。この例ではまず鍵情報 Key から疑似乱数系列  $\{r_{i,j}\}$  を生成してステップ S 2 に移る (S 8)、またステップ S 4 の次に電子透かし系列に対し疑似乱数系列  $\{r_{i,j}\}$  で復調を行ってステップ S 5 へ移る (S 9)。ステップ S 5 の判定式 (4) 中の透かしビット  $b'$

$i, j$  はステップ S9 で復調したものであり、同様にステップ S6 での多数決処理もステップ S9 で復調した  $b'_{i,j}$  について行う。

#### 実施例 5

疑似乱数系列によって透かし情報を拡散しているため、 $q$  を  $1/2$  に近似すると、透かし系列が透かしありか否かの判定を次のようにすることもできる。

【0035】

電子透かしの各ビット情報を構成する  $n$  ビットの透かし系列にビット '1' が  $x$  個含まれる確率は、二項分布関数  $F(x)$  を用いて、

$$F(x) = \sum_{j=0}^x {}_n C_j (1/2^n)$$

と表せる。これより予め、

$$F(x = x_1) \geq \alpha$$

を満たす最小の整数  $x_1$  を求めておくことにより、実施例 4 の Step 5. を透かし系列を疑似乱数系列で復調した系列について下記式 (6) で判定できる。この場合は多数決判定と同程度の計算量に軽減することが可能である。

【0036】

【数 4】

$$\frac{\sum_{i=0}^{m-1} \left| \sum_{j=0}^{n-1} b'_{i,j} - \frac{n}{2} \right|}{m} + \frac{n}{2} \geq x_1 \quad \dots\dots (6)$$

この判定は透かし系列の二項分布の中心  $n/2$  からの偏より度合の平均が  $x_1$  以上であるかを判定していることになる。

式 (6) が成立して透かし有りとは判定されると、すべての  $0 \leq i < m$  について、透かし系列を疑似乱数系列で復調したものを、下記のように多数決処理して、

$$\sum_{j=0}^{n-1} b'_{i,j} < n/2 \text{ のとき: } w'_i = 0$$

$$\sum_{j=0}^{n-1} b'_{i,j} > n/2 \text{ のとき: } w'_i = 1$$

透かし情報を再構成する。また、

【0037】

【数5】

$$\frac{\sum_{i=0}^{m-1} \left| \sum_{j=0}^{n-1} b'_{i,j} - \frac{n}{2} \right|}{m} + \frac{n}{2} < x_1$$

のときは、透かし無しもしくは不明と判定する。

$F(x=x_1) \geq \alpha$  を満す最小の整数  $x_1$  を用いる代りに、 $F(x=x_0) \leq 1-\alpha$  を満す最大の整数  $x_0$  を求めて処理してもよい。この場合の透かしがあるかの判定式は下記の式(7)となる。

【0038】

【数6】

$$\frac{n}{2} - \frac{\sum_{i=0}^{m-1} \left| \sum_{j=0}^{n-1} b'_{i,j} - \frac{n}{2} \right|}{m} \leq x_0 \quad \dots\dots (7)$$

この式の左辺が  $x_0$  より大きければ透かし無し又は不明と判定する。

#### 実施例 6

式(4)により透かしありと判定した場合に、前記多数決処理により電子透かし情報を再構成すると共に、その再構成された透かし情報の系列の全体についての信頼度として、

【0039】

【数7】

$$F\left(\frac{\sum_{i=0}^{m-1} \left| \sum_{j=0}^{n-1} b'_{i,j} - \frac{n}{2} \right|}{m} + \frac{n}{2}\right)$$

を計算して出力する。

同様に式(5)により透かしありと判定した場合で、電子透かし情報を再構成

した場合は、その透かし情報の系列の全体についての信頼度として

【0 0 4 0】

【数 8】

$$F \left( \frac{n}{2} - \frac{\sum_{i=0}^{m-1} \left| \sum_{j=0}^{n-1} b'_{i,j} - \frac{n}{2} \right|}{m} \right)$$

を計算して出力する。

また式（6）により透かしありと判定した場合に、前記した多数決処理により電子透かし情報を再構成すると共にその透かし情報の系列の全体についての信頼度として、

【0 0 4 1】

【数 9】

$$F \left( \frac{\sum_{i=0}^{m-1} \left| \sum_{j=0}^{n-1} b'_{i,j} - \frac{n}{2} \right|}{m} + \frac{n}{2} \right)$$

を計算して出力する。

同様に式（7）により透かしありと判定した場合は、その透かし情報の系列の全体についての信頼度として

【0 0 4 2】

【数 1 0】

$$F \left( \frac{n}{2} - \frac{\sum_{i=0}^{m-1} \left| \sum_{j=0}^{n-1} b'_{i,j} - \frac{n}{2} \right|}{m} \right)$$

を計算して出力する。

実施例 1 乃至 6 においてビット 1 の抽出確率および個数を用いたが、ビット 0 の抽出確率および個数を用いても実装上の違いのみで、本質的に変わらない。

以下は実験例を示す。

#### 【0043】

実験対象画像として128×128画素の“lena”画像を用い、信頼度のしきい値 $\alpha$ を0.999999として実験を行なった。

#### 実験1

1ビットの透かし情報“1”を秘密鍵情報“50, 000”を用いて127回繰り返し埋め込み、任意の秘密鍵情報を用いて透かし系列の読みとりを行なった。図9は、秘密鍵情報に対する読みとり透かし系列のビット1の個数を示したものである。縦軸は読みとった透かし系列におけるビット1の個数、横軸は秘密鍵情報の値を表している。ただし、透かし対象領域Aのビット1の出現頻度は $q = 0.492247$ であった。正しい秘密鍵(50, 000)を用いた場合、ビット1の個数が透かし有無の判定しきい値 $\times_1$ より大きいことから、正当率99.9999%で透かし情報は1であると判定でき、正しくない秘密鍵を用いた場合はすべて透かし無しもしくは不明と判定した。

#### 実験2

7段のM系列(初期状態64)を用いて変調した透かし系列を埋め込み、任意の秘密鍵情報と初期状態が任意のM系列を用いて実験1と同様の実験を行なった(図10)。変調を行なうことにより、実験1のデータと比較して $q$ の値は0.500000に、分散は31.008265から31.718777とほとんど変化しなかった。透かしが抽出できたのは、正しい秘密鍵情報と疑似乱数系列の組を用いたときのみであった。また、透かし対象領域Aの半分のデータに透かし系列を埋め込んだ場合、変調なしでは $q = 0.741547$ であったのに対し、変調を行なうことで $q = 0.499768$ という結果が得られた。

#### 【0044】

##### 【発明の効果】

1. 統計学における二項分布に基づき電子透かし情報を判定することにより以下の効果がある。

－電子透かしが入っていない情報コンテンツを電子透かし有りと判定したり、電子透かしが入っている情報コンテンツから正しくない電子透かしを抽出する確

率を定量的に評価でき、その値を電子透かしの信頼度のしきい値  $\alpha$  を用いて  $2(1 - \alpha)$  で抑えることができる。

【0045】

2. 電子透かし情報を埋め込む前に疑似乱数系列で変調することにより以下の効果がある。

－電子透かし情報の全埋め込み対象領域から任意の1ビット電子透かし系列を抽出したときにビット1が抽出される確率  $q$  の偏りを無くした。

－電子透かし抽出に必要な正しい電子透かしの秘密鍵情報と抽出した電子透かし系列を復調するのに必要な疑似乱数系列無しに  $q$  の偏りから電子透かしの有無ならびにその値を検知することが困難となった。これは電子透かしシステムで重要な要素であるセキュリティの強化につながることである。

【0046】

－実装において、 $q = 1/2$  と仮定できるため、電子透かし情報再構成処理は多数決処理と同程度の計算量となり、処理の高速化が図れる。

$\alpha$  は、抽出した情報の正当率の下限を示す指標であり、電子透かしシステムの内部で管理可能な情報となっている。これは、従来の電子透かしシステムに見られた、抽出した電子透かし情報の正当率を利用者に提示するものより優れている。

【0047】

実施例1では、透かし情報  $\{w'_i\}$  を構成するビット情報のうち1ビットでも信頼度が低いものがある場合、透かし情報無しもしくは不明と判定する。しかしながら、このような場合でも、実施例4～6では透かし系列  $\{b'_{i,j}\}$  , ( $0 \leq i < m$ ,  $0 \leq j < n$ ) 全体を統計的に見ると、透かし情報を十分再構成することができる場合が多いことから、透かし情報の有無を判定する式を改良し、透かし情報の全体を統計的処理をしたものとするにより、透かし情報を構成するビット情報のうち数ビット信頼性が低いビットがある場合にでも、透かし情報の信頼性を定量的に評価し、その値を  $2(1 - \alpha)$  で抑えることができ、かつ透かし情報を再構成することができる。また、実施例1では電子透かし系列から電子透かし情報を再構成するのに、すべての  $i$  に対して二項分布の分布関数  $F(x$

)を用いて、 $F(\sum_{j=0}^{n-1} b'_{i,j})$ の値を計算する必要があったが、実施例 4～6 では分布関数を用いた計算を 1 回にすることができ、透かしの再構成にかかる計算量を軽減できる。

【0 0 4 8】

この発明は、誤り訂正符号と併用することでさらに大きな効果が得られる。すなわち、電子透かし情報の一部のビットだけが集中して壊れているような場合、抽出した情報は、一部のビットだけが不明で、それ以外のビット情報は正当性が高い状態にあると正確に判定できる。よって壊れたビット情報のみを誤り訂正することにより、確実に正しい情報が抽出できる。

【図面の簡単な説明】

【図 1】

電子透かしシステムの概要を示す図。

【図 2】

図 1 中の電子透かし抽出装置概要を示す図。

【図 3】

電子透かし情報の判定を示す図。

【図 4】

電子透かし情報再構成の概念を示す図。

【図 5】

電子透かし抽出処理の手順を示す図。

【図 6】

この発明の第 2 実施例の概要を示す図。

【図 7】

この発明の第 4 実施例の処理手順を示す流れ図。

【図 8】

この発明の第 4 実施例に対し、疑似乱数変調透かし情報の埋め込みを対象とした場合の処理手順を示す流れ図。

【図 9】

透かし系列読みとり結果（変調なし）を示す図。

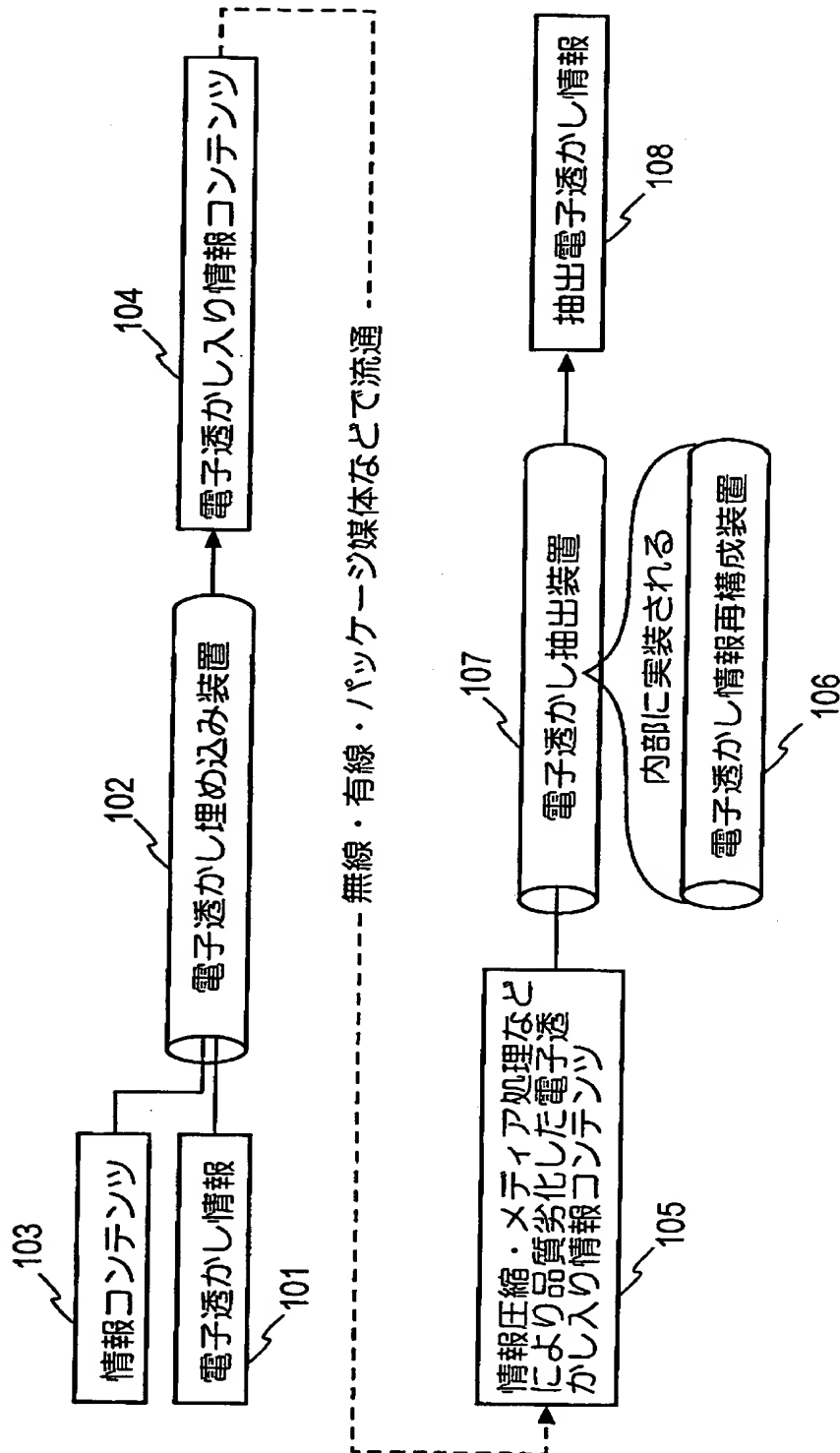
【図 10】

透かし系列読みとり結果（変調あり）を示す図。



【書類名】 図面

【図1】



【図 2】

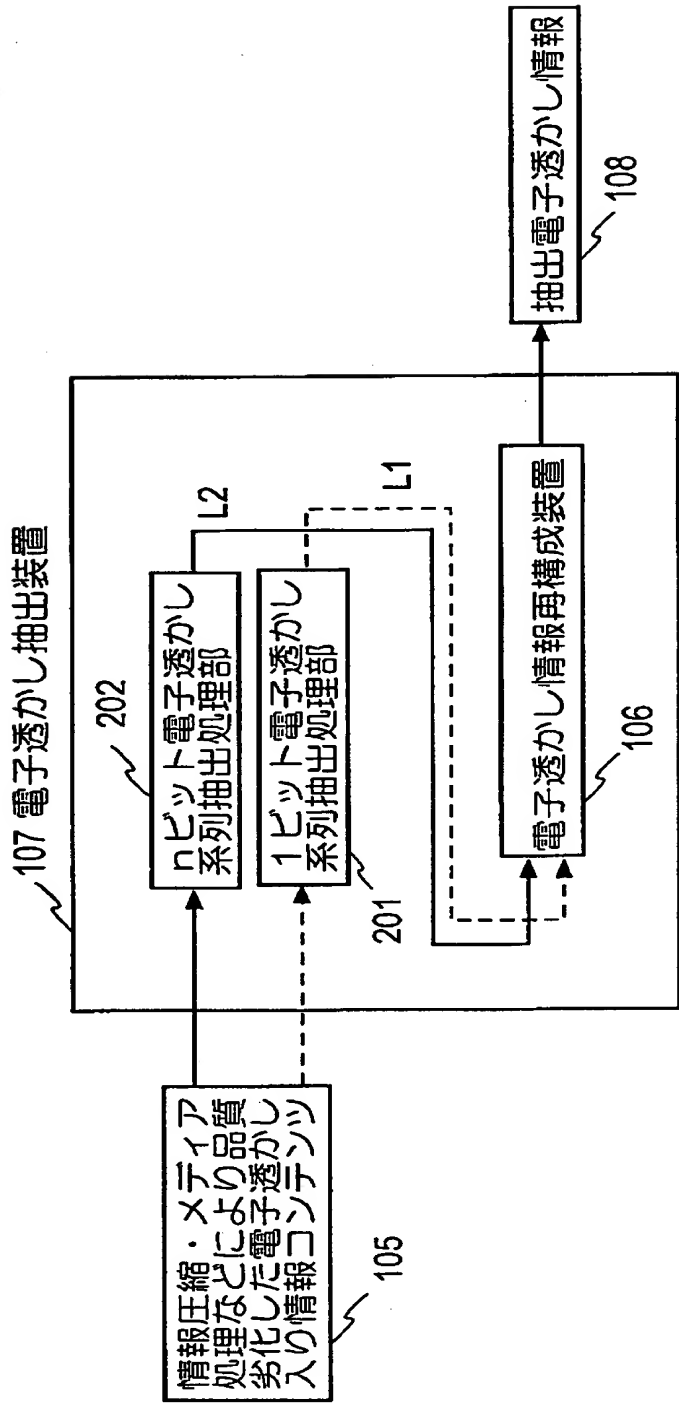


図 2

【図 3】

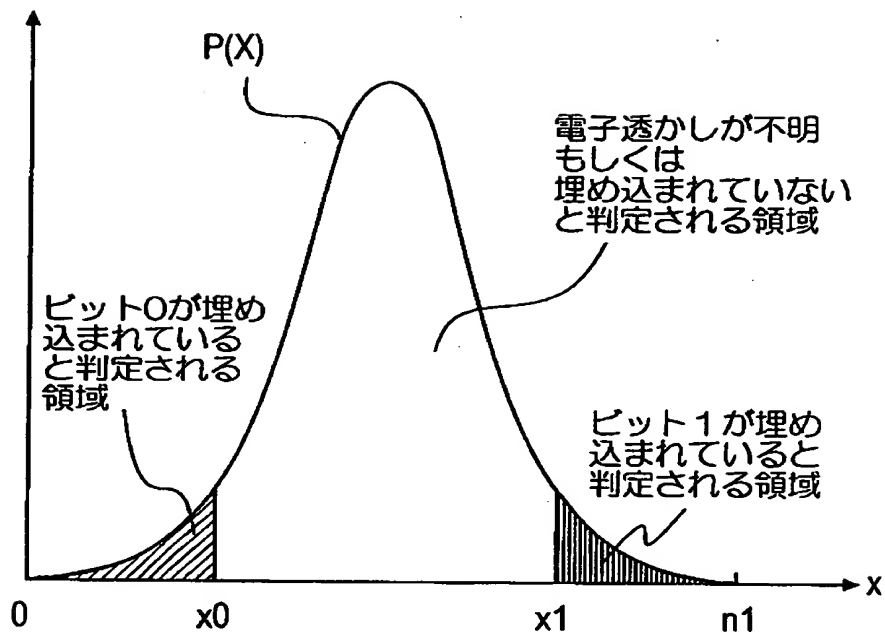


図 3

【図 4】

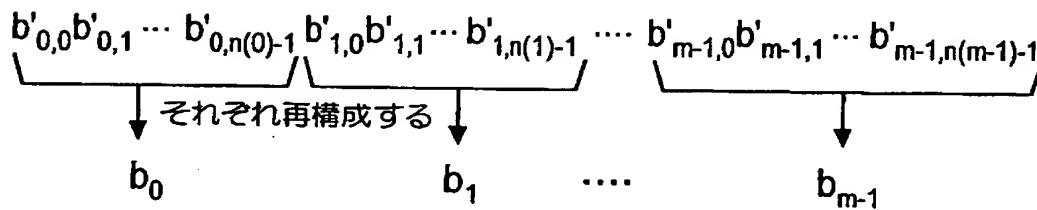
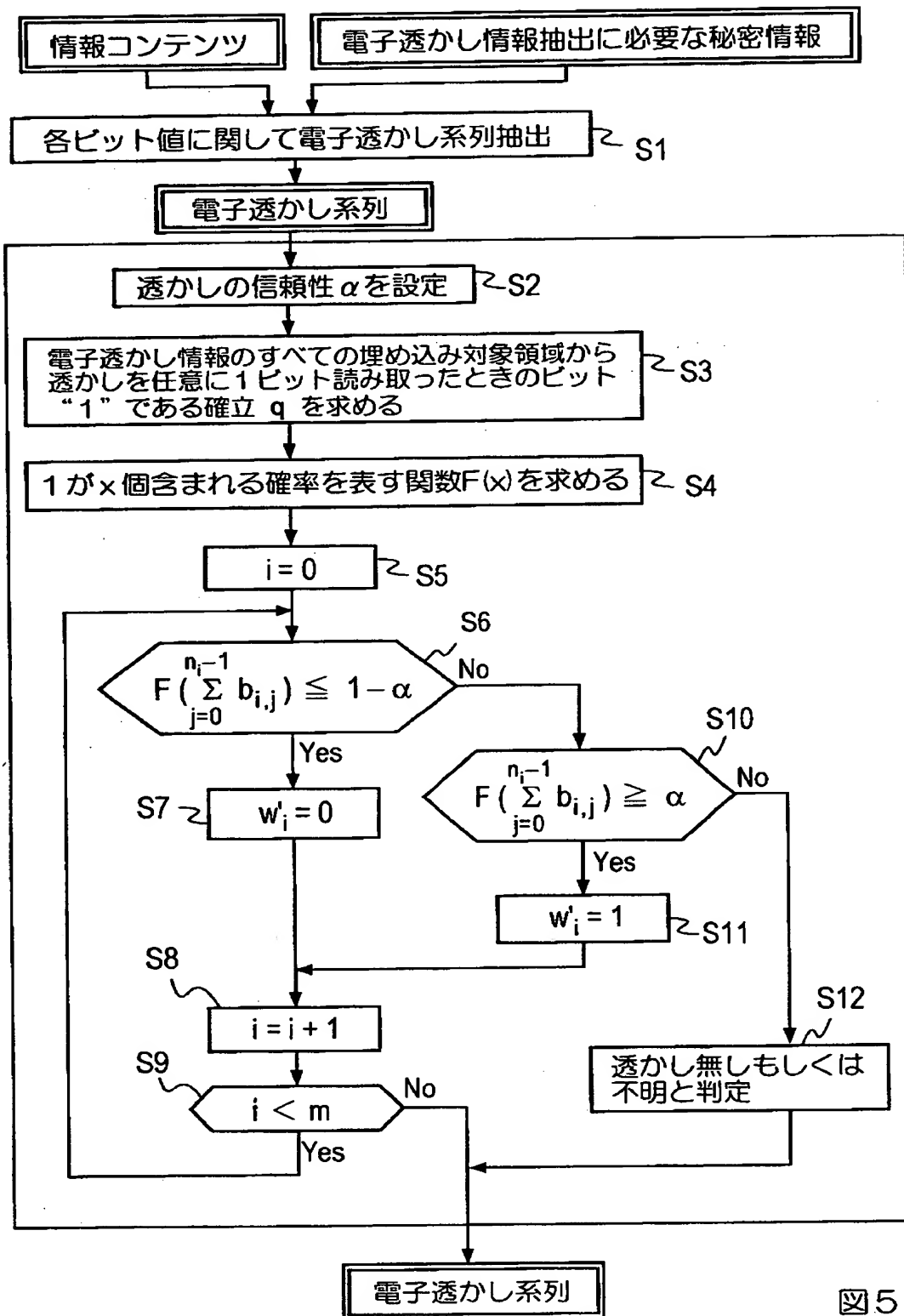


図 4

【図 5】



【図 6】

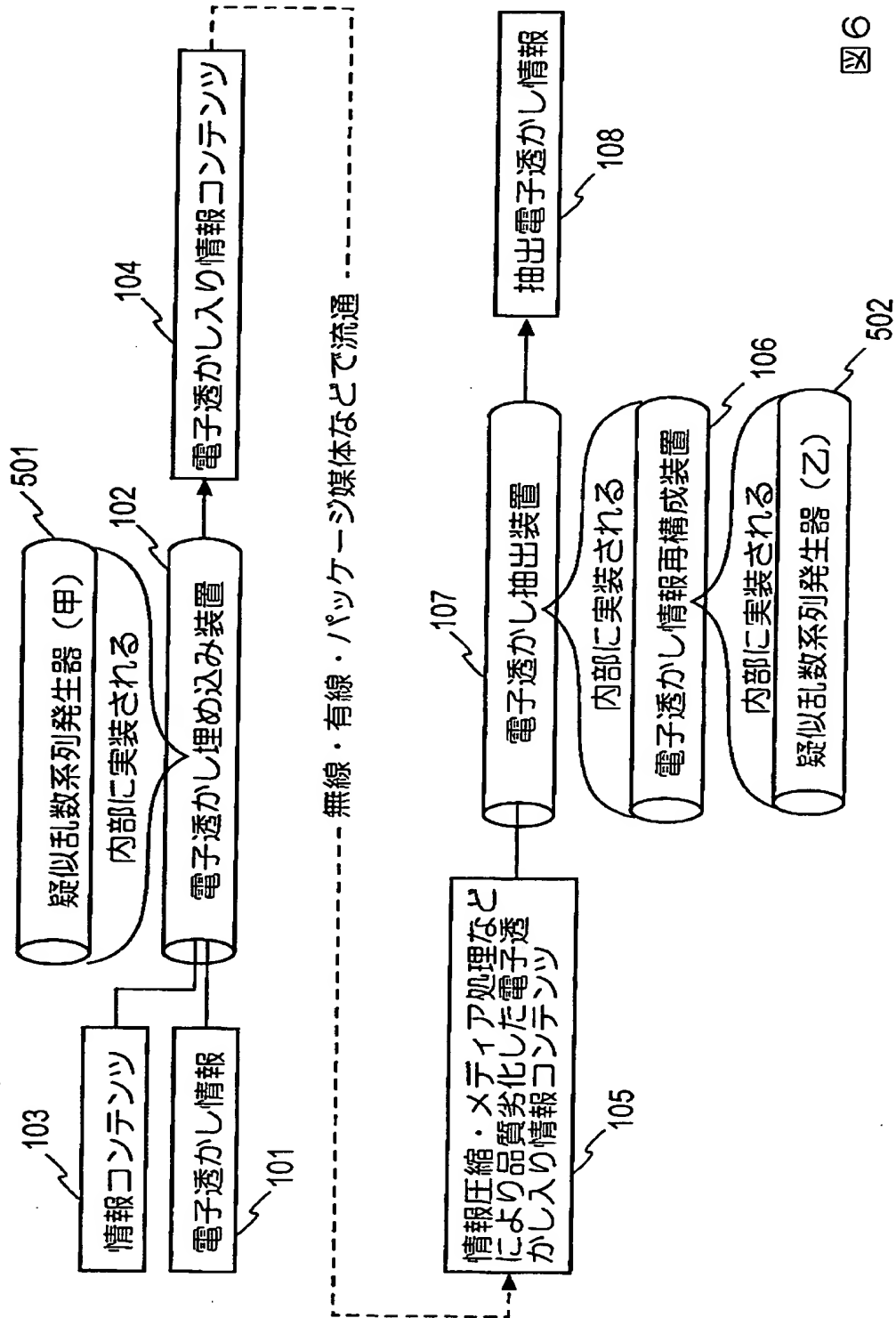


図 6

【図 7】

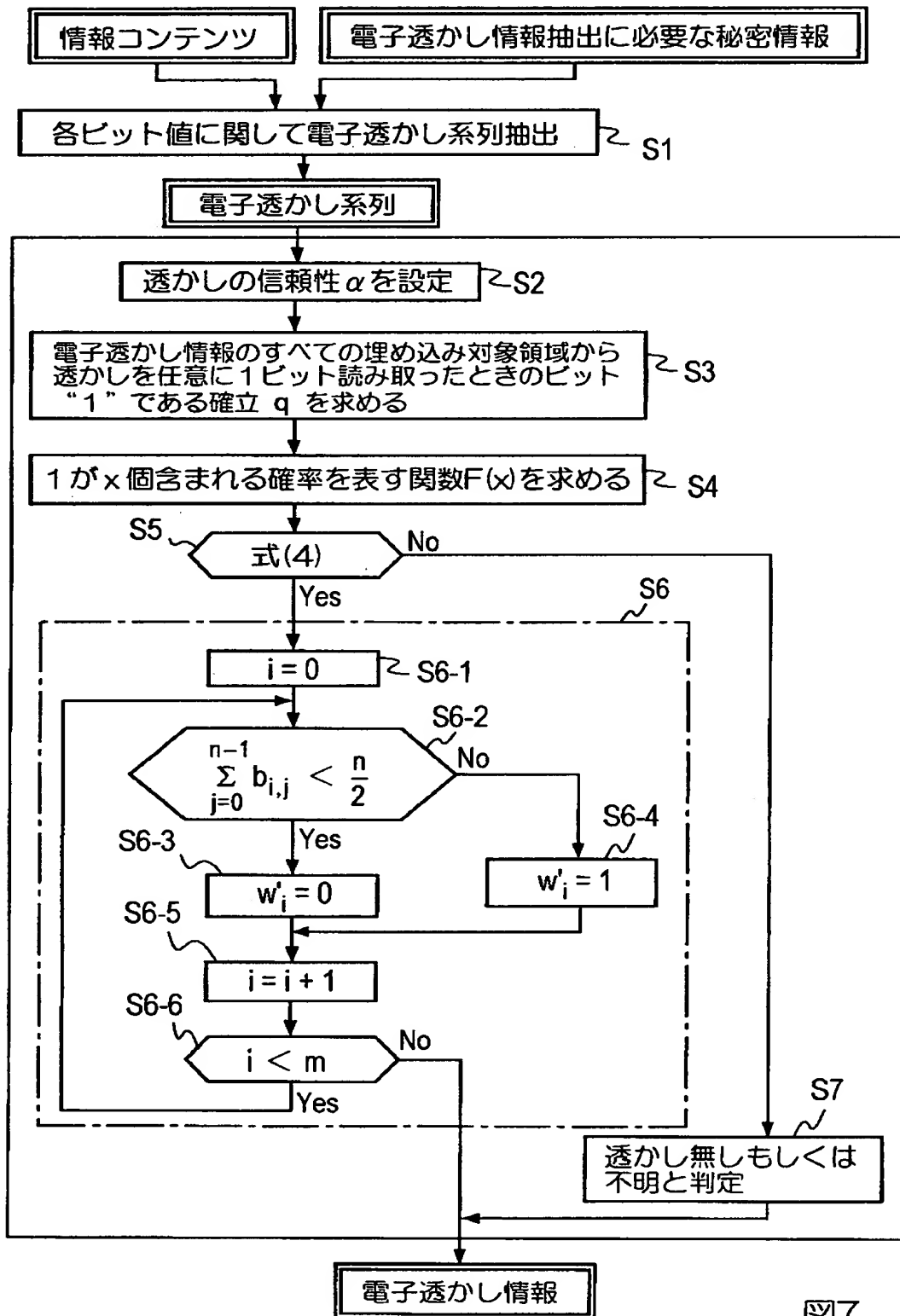


図 7

【図 8】

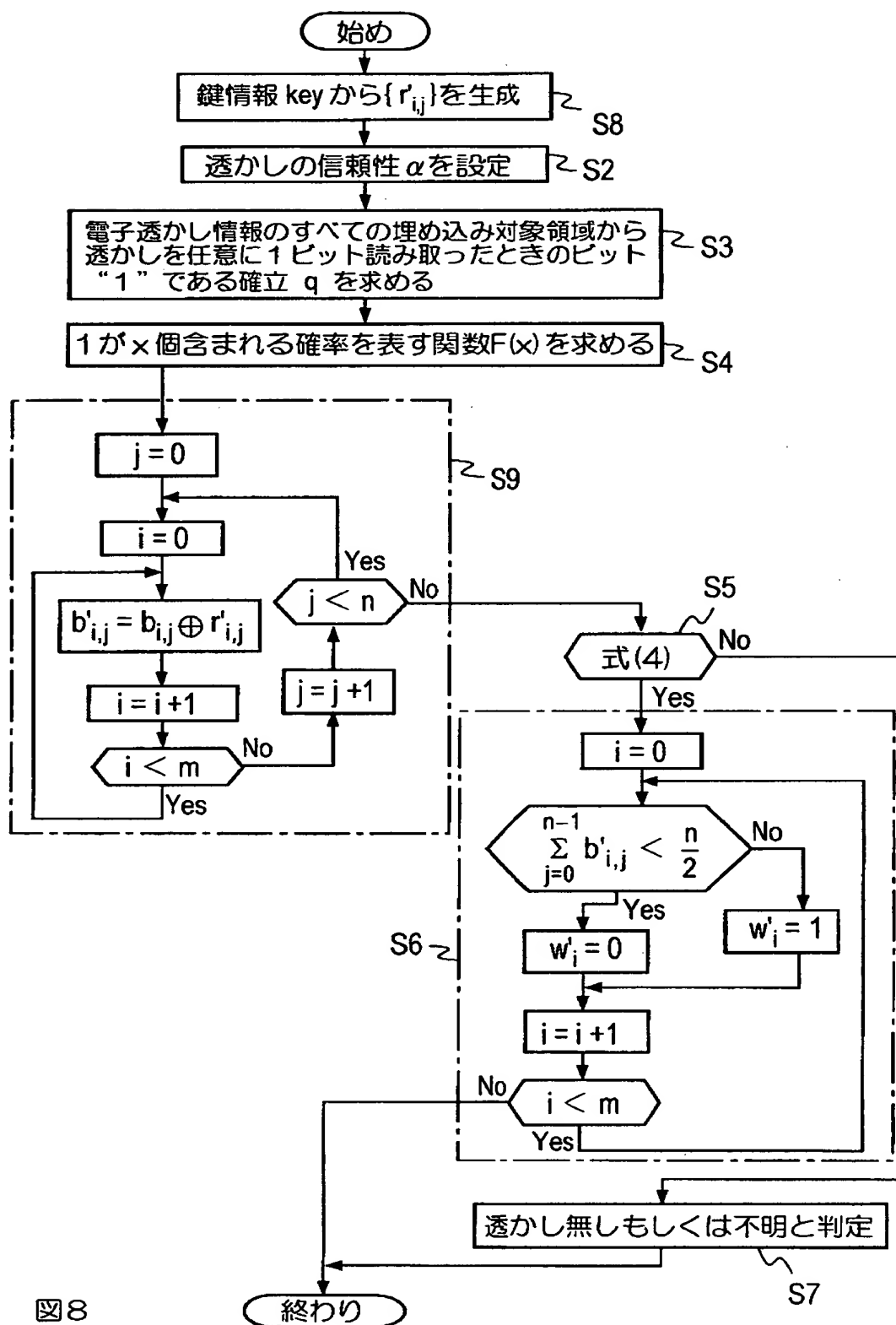


図 8

【図 9】

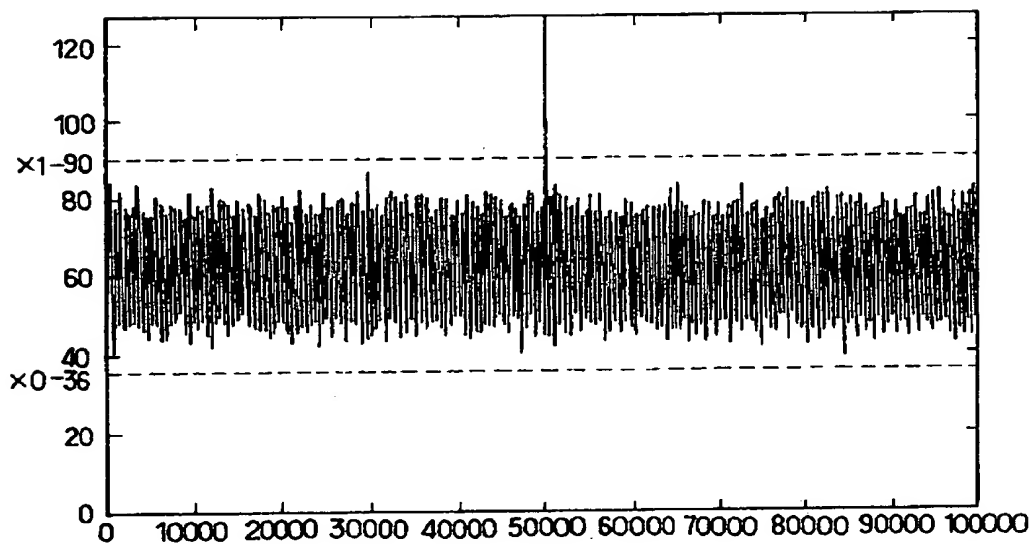


図 9

【図 10】

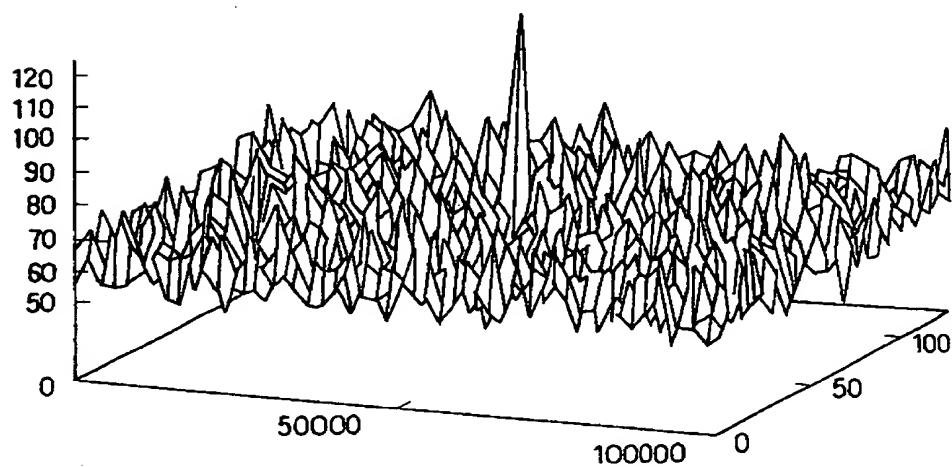


図 10



【書類名】 要約書

【要約】

【課題】 電子透かしが入っている情報コンテンツから正しくない電子透かしを抽出する確率を定量的に評価する。

【解決手段】 情報コンテンツの透かし対象領域から無作為に 1 ビット透かし系列の抽出を行い、その時のビット 0 と 1 の出現確率  $1-q$  と  $q$  を求め、透かしが埋め込まれたのべ回数  $n_i$  ビットだけ透かし系列を抽出し、この時、 $n_i$  ビット列に 1 が  $k$  個現れる確率

$$P(x=k) = n_i C_k q^k \cdot (1-q)^{n_i-k}$$

その分布関数

$$F(x) = \sum_{k=0}^x n_i C_k q^k \cdot (1-q)^{n_i-k} \quad (0 \leq x \leq n_i)$$

より、透かし情報の信頼度のしきい値  $\alpha$  ( $1/2 < \alpha \leq 1$ ) に対し、 $0 \leq F(x=x_0) \leq 1-\alpha$  を満す最大の  $x_0$  と、 $\alpha \leq F(x=x_1) \leq 1$  を満す最小の  $x_1$  をそれぞれ透かし情報判定しきい値とする。

【選択図】 図 3

認定・付加情報

特許出願の番号	平成11年 特許願 第118072号
受付番号	59900400273
書類名	特許願
担当官	第七担当上席 0096
作成日	平成11年 5月 6日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000004226
【住所又は居所】	東京都新宿区西新宿三丁目19番2号
【氏名又は名称】	日本電信電話株式会社

【代理人】

申請人

【識別番号】	100066153
【住所又は居所】	東京都新宿区新宿四丁目2番21号 相模ビル
【氏名又は名称】	草野 卓

【選任した代理人】

【識別番号】	100100642
【住所又は居所】	東京都新宿区新宿4丁目2番21号 相模ビル 草野特許事務所
【氏名又は名称】	稲垣 稔

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日 1995年 9月21日  
[変更理由] 住所変更  
住 所 東京都新宿区西新宿三丁目19番2号  
氏 名 日本電信電話株式会社
2. 変更年月日 1999年 7月15日  
[変更理由] 住所変更  
住 所 東京都千代田区大手町二丁目3番1号  
氏 名 日本電信電話株式会社